**Рекомендации по безопасности сайтов структур ФНПР**

**Основные способы защиты сайтов от атак**

Атаки на сайты производятся как целенаправленно, так и с помощью бот-сетей автоматизированно. Как правило, каждая атака имеет свою стоимость. И если автоматизированные атаки при всей своей массовости эффективны, от них можно достаточно легко оградиться, соблюдая несколько простых правил. В случае целенаправленной атаки целесообразнее потерять контроль над сайтом и восстановить его заново, чем сражаться за его работоспособность, расходуя серьезные ресурсы.

Тем не менее, соблюдая простые рекомендации, в большинстве случаев сайты сохраняют свою работоспособность даже в сложных условиях.

Итак, что можно сделать для защиты сайтов:

- использовать надежный хостинг;

- подключить SSL-сертификат;

- обеспечить защиту от DDoS-атак;

- использовать безопасные плагины/библиотеки/фреймворки/CMS;

- применять техники защиты от SQL-инъекций и XSS-атак;

- обеспечить ведение журнала веб-сайта и мониторинг событий безопасности;

- производить регулярное резервное копирование веб-сайта и всех важных данных;

- использовать надежные и сложные пароли, а также защиту от перебора паролей;

- необходимо изменить стандартный адрес входа и обеспечить контроль доступа к административной панели сайта.

При создании сайта, его обновлении или в процессе администрирования стоит избегать покупки или размещения сайта на серверах организации, виртуальных серверах и на самостоятельно администрируемых серверах в дата-центрах. Такое решение, безусловно, жизнеспособно, но требует высокого профессионального уровня технических специалистов и серьезных вложений.

**Доменное имя**

Доменное имя необходимо приобретать отдельно, используя официальные ресурсы регистраторов доменов (nic-ru, ru-center.ru), регистрация доменного имени должна производиться на юридическое лицо с указанием официальных контактов организации, в том числе в качестве администратора. Такое решение позволит избежать утери данных, потери управления и кражи домена даже в случае смены администратора.

В панели управления регистратора домена проводятся настройки DNS-серверов, почтовых сервисов и другие базовые настройки доменов. Здесь же можно заказать SSL-сертификат для сайта и услуги по его запуску.

**!** Необходимо избегать решений «все в одном». Нельзя совмещать почтовые сервисы, сервисы и ресурсы сайта в одном личном кабинете.

**Хостинг-провайдер**

При выборе хостинг-провайдера необходимо обратить внимание на то, предоставляет ли провайдер услуги по защите от DDoS-атак или установлен ли кеширующий прокси - Nginx. В случае с Nginx необходимо обратить внимание на возможность настройки и настройки по умолчанию. Все возможные и предлагаемые провайдером средства безопасности должны быть включены, оплачены и настроены. Просмотр журналов безопасности должен проводиться регулярно. При увеличении числа атак или событий безопасности необходимо проводить соответствующую настройку систем безопасности. В случае оповещения провайдером о наличии опасности необходимо незамедлительно принять соответствующие меры.

**!** Пароли к панели управления (как и все пароли, связанные с работой или администрированием сайта) должны быть максимально устойчивы к подбору, должны содержать буквы верхнего и нижнего регистров, цифры, специальные символы и иметь длину не менее 11 знаков.

Пароль администратора с полным доступом к ресурсам должен быть только у ответственного лица, находящегося в штате организации.

**Фреймворки, CMS, "Движки" сайтов**

Для работы сайта, как правило, выбираются популярные системы управления. Важно понимать:

- следует избегать кустарных и «самописных» систем управления;

- следует избегать систем управления, работающих по подписке;

- следует избегать сервисов-конструкторов сайтов;

- для работы сайта можно выбирать популярные бесплатные CMS при условии соблюдения строгих правил;

- необходимо постоянно поддерживать версию системы управления сайтом в актуальном состоянии, регулярно обновлять как саму CMS, так и компоненты (плагины, модули, приложения);

- не поддерживаемые или прекратившие свою работу дополнения к системе управления необходимо заменять на актуальные;

- при самостоятельном создании модификаций на сайте нельзя применять их, отключая системы безопасности, или применять небезопасные настройки хостинга и системы управления;

- при подключении баз данных к сайтам необходимо использовать устойчивые пароли как к самими базам данных, так и к системам, с которыми они работают;

- крайне желательно устанавливать дополнительные плагины и системы, обеспечивающие безопасность системы управления сайтом.

**Резервное копирование**

Необходимо настроить несколько видов резервного копирования:

Регулярное (желательно еженедельное) резервное копирование средствами хостинг-провайдера всех ресурсов сайта (единый архив сайта). Такое копирование настраивается в административной панели хостинг-провайдера и происходит автоматически, сохраняясь на стороне хостинг-провайдера. Такой архив поможет восстановить работоспособность сайта в течение нескольких часов.

Регулярное копирование на компьютер администратора сайта. Перед каждым изменением, вносимым в работу сайта, администратор должен сохранить на рабочем компьютере резервную копию всех ресурсов сайта (базы данных, файлы, папки, скрипты и файлы конфигурации). Также такое копирование должно происходить ежемесячно. Такое копирование позволит восстановить сайт даже в случае необходимости переместить сайт в более безопасное пространство.

Резервное копирование баз данных. Используя инструменты администрирования баз данных, с периодичностью раз в неделю необходимо копировать базы данных сайта на специально выделенные для этого ресурсы (это могут быть как ресурсы хостинг-провайдера, так и аккаунты на облачных ресурсах). Это позволит восстановить сайт даже при массированной атаке и утрате всех возможностей для восстановления.

**Администрирование сайта**

При использовании любых систем управления сайтом рекомендуется изменять стандартную страницу входа в панель администрирования. На странице входа администратора необходимо использовать помимо стандартных данных (логин и пароль) системы наподобие captcha или двухфакторную аутентификацию. Следует избегать запоминания пароля менеджерами паролей на компьютерах администраторов и всех работающих с сайтом сотрудников.

Необходимо разделять учетные записи пользователей, редакторов, авторов и администраторов сайта. Если сайт «ведется» администратором, то для ежедневной работы должна использоваться учетная запись с ограниченным функционалом. Учетных записей администратора должно быть две: основная и резервная. Не допускается загружать на сайт файлы, не прошедших проверку антивирусом или файлы скриптов. Также в панели администратора необходимо прописать типы файлов для загрузки и их максимальный размер.

Пароли к панели управления (как и все пароли, связанные с работой или администрированием сайта) должны быть максимально устойчивы к подбору, должны содержать буквы верхнего и нижнего регистров, цифры, специальные символы и иметь длину не меньше 11 знаков.

Пароль администратора с полным доступом к ресурсам должен быть только у ответственного лица, находящегося в штате организации.

Департамент по связям с общественностью, молодежной политике и развитию профсоюзного движения аппарата ФНПР